

Modül 8: Ağ Katmanı

Introduction to Networks v7.0
(ITN)



Modül 8: Konular

Bu modülde ne öğreneceğim?

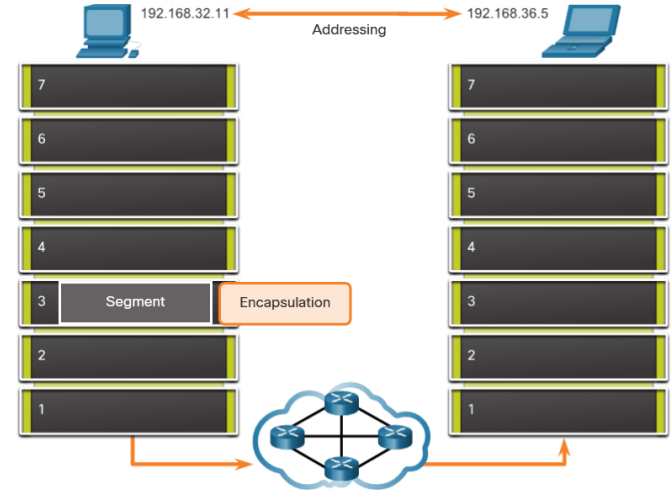
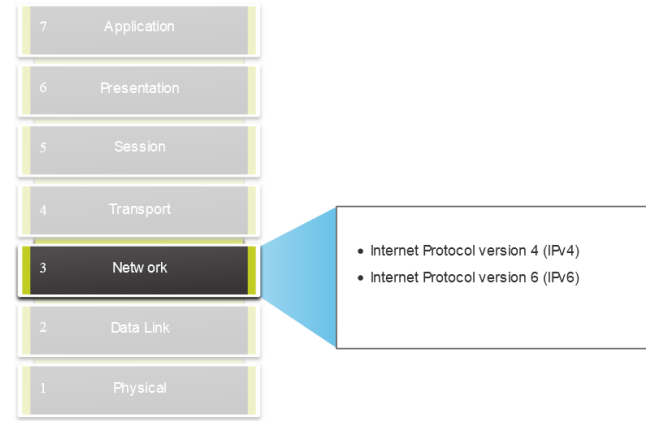
Konu Başlığı	Konu Amacı
Ağ Katmanı Özellikleri	Ağ katmanının güvenilir iletişim için IP protokollerini nasıl kullandığını açıklayın.
IPv4 Paketi	IPv4 paketindeki ana başlık alanlarının rolünü açıklayın
IPv6 Paketi	IPv6 paketindeki ana başlık alanlarının rolünü açıklayın
Yönlendiriciler nasıl barındırılır?	Ağ cihazlarının paketleri bir hedef ağa yönlendirmek için yönlendirme tablolarını nasıl kullandığını açıklayın.
Router Yönlendirme Tabloları	Bir yönlendiricinin yönlendirme tablosundaki alanların işlevini açıklayın.

8.1 Ağ Katmanları Özellikleri

Ağ Katmanı Özellikleri

Ağ Katmanı

- Uç cihazların veri alışverişi yapmasına izin veren hizmetler sağlar
- IP version 4 (IPv4) and IP version 6 (IPv6) temel ağ katmanı iletişim protokolleridir.
- Ağ katmanı dört temel işlemi gerçekleştirir:
 - Uç cihazları adresleme
 - Kapsülleme (Encapsulation)
 - Yönlendirme (Routing)
 - Kapsül açma (De-encapsulation)



Network layer protocols forward transport layer PDUs between hosts.

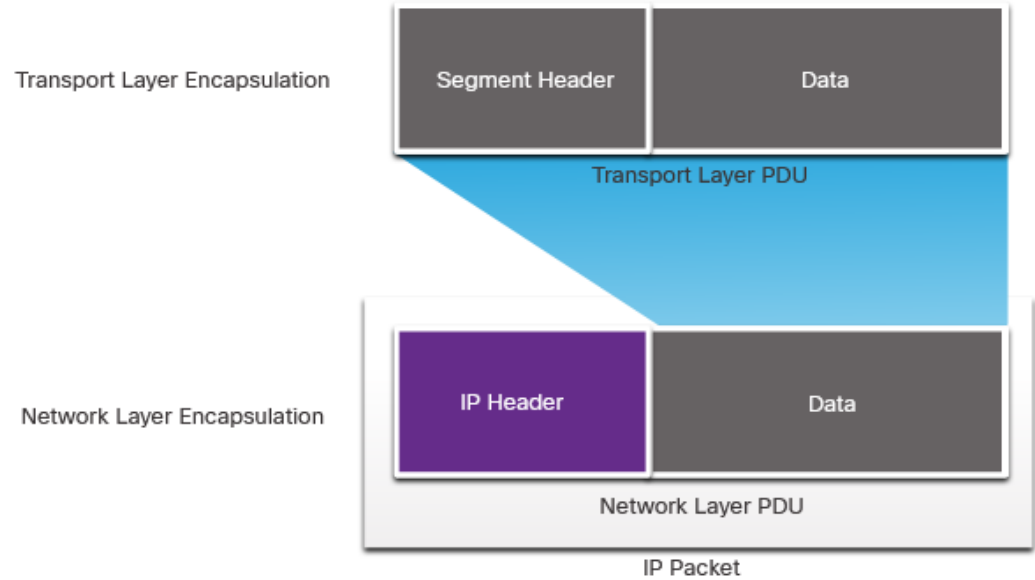
© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ağ Katmanı Özellikleri

IP Kapsülleme

- IP, taşıma katmanı segmentini kapsüller.
- IP, IPv4 veya IPv6 paketini kullanabilir ve katman 4 segmentini etkilemez.
- IP paketi, ağı geçerken tüm 3. katman cihazları tarafından incelenir.
- IP adresleme kaynaktan hedefe değişmez.

Not: NAT adreslemeyi değiştirecektir, bu konu ileriki modülde anlatılacaktır.



Ağ Katmanı Özellikleri

IP'nin Özellikleri

IP'nin en düşük ek yüke sahip olması amaçlanmıştır ve şu şekilde tanımlanabilir:

- Bağlantısız
- En iyi çaba
- Medyadan bağımsız

Ağ Katmanı Özellikleri

Bağlantısız

IP bağlantısızdır.

- IP, paketi göndermeden önce hedef ile bağlantı kurmaz.
- Gerekli kontrol bilgisi (senkronizasyonlar, onaylar, vb.) yoktur.
- Hedef ulaştığında paketi alacaktır, ancak IP tarafından ön bildirim gönderilmez.
- Bağlantı yönelimli trafiğe ihtiyaç varsa, bunu başka bir protokol gerçekleştirecektir (tipik olarak taşıma katmanındaki TCP).



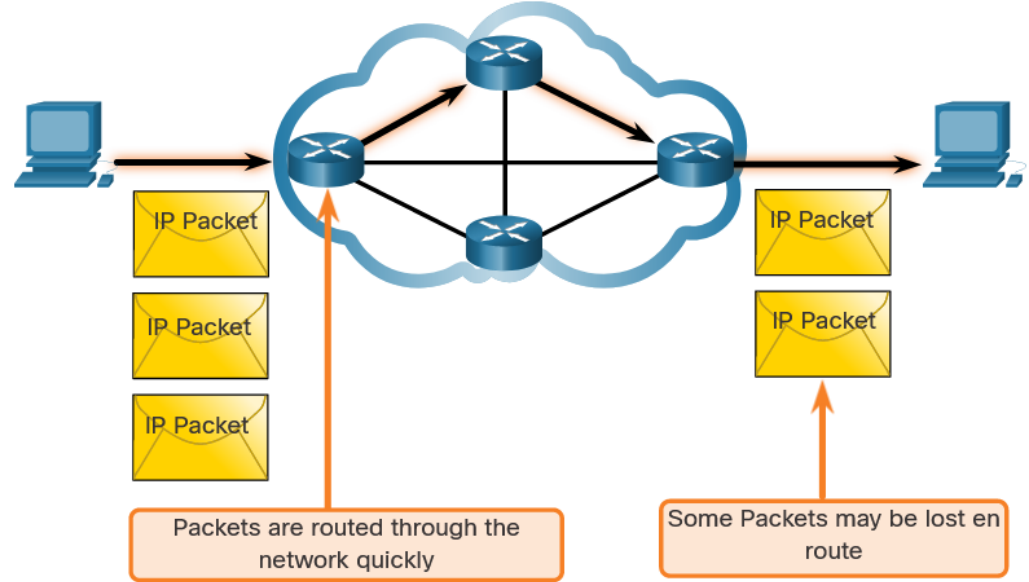
A letter is sent.

Ağ Katmanı Özellikleri

En iyi çaba

IP en iyi çabadır.

- IP, paketin teslimini garanti etmez.
- Alınmayan verileri yeniden gönderecek bir mekanizma olmadığı için IP ek yükü azaltır.
- IP onay beklemez.
- IP diğer cihazın çalışıp çalışmadığını veya paketi alıp almadığını bilmez.



Ağ Katmanı Özellikleri

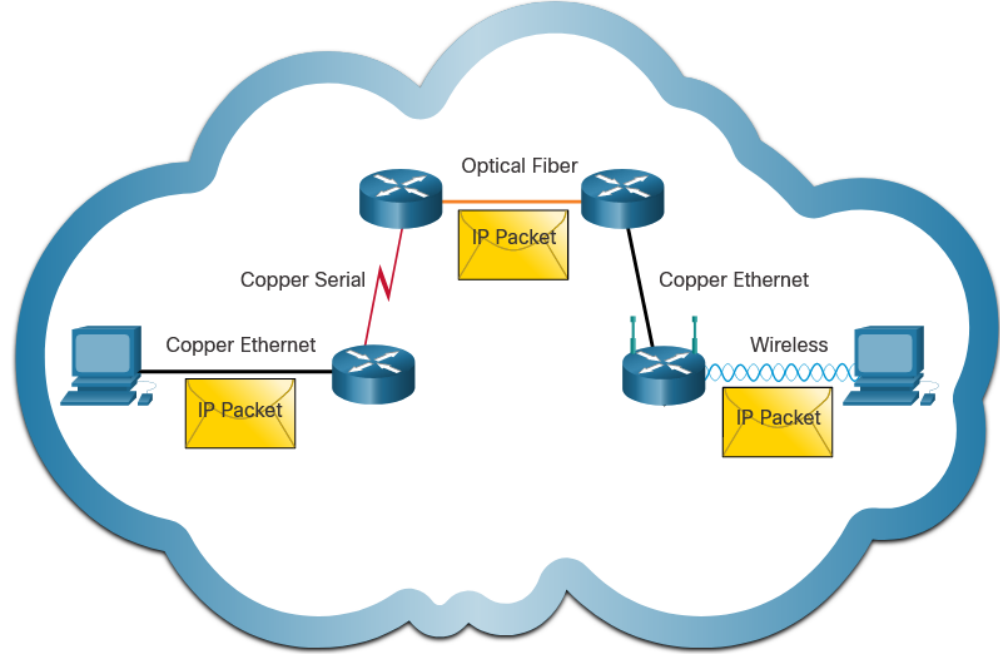
Medyadan Bağımsız

IP güvenilmezdir:

- Teslim edilmeyen veya bozuk paketleri yönetemez veya düzeltemez.
- Bir hatadan sonra IP yeniden iletilemez.
- IP, sıradan çıkmış paketleri yeniden düzenleyemez.
- IP, bu işlevler için diğer protokollere güvenmelidir

IP medyadan bağımsızdır:

- IP, veri bağlantı katmanında gereken çerçeve türü veya fiziksel katmandaki ortam türü ile ilgilenmez.
- IP, herhangi bir ortam türü üzerinden gönderilebilir: bakır, fiber veya kablosuz.



Medyadan Bağımsız (devamı)

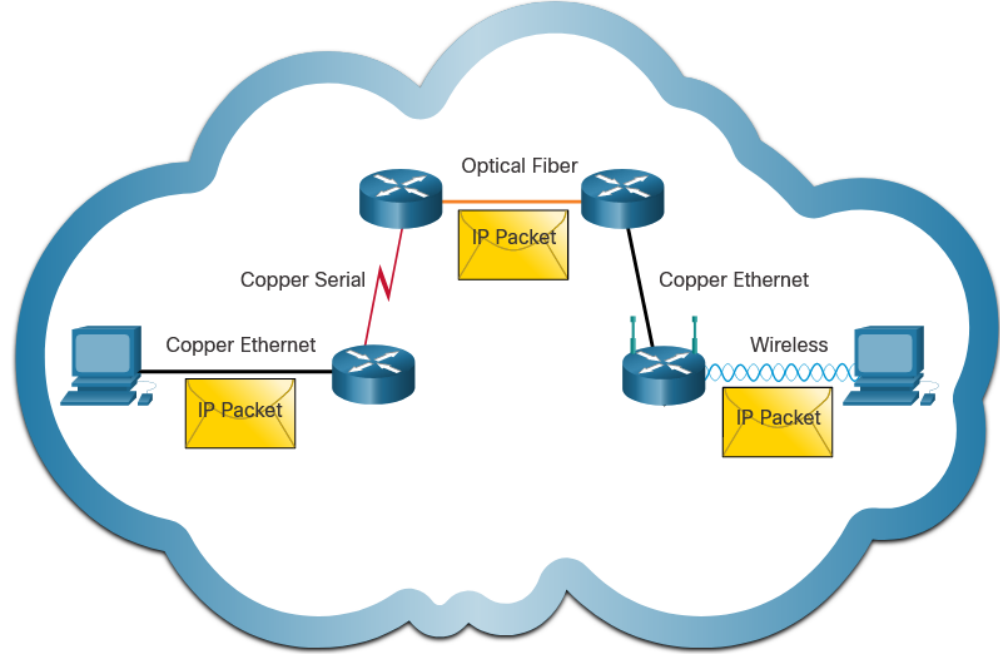
Ağ katmanı Maximum Transmission Unit (MTU)'i kurar.

- Ağ katmanı, bunu veri bağlantı katmanı tarafından gönderilen kontrol bilgilerinden alır.
- Ağ daha sonra MTU boyutunu belirler.

Parçalanma, Katman 3'ün IPv4 paketini daha küçük birimlere ayırmasıdır.

- Parçalanma gecikmeye neden olur.
- IPv6 paketleri parçalamaz.
- Örnek: Yönlendirici, Ethernet'ten daha küçük MTU'ya sahip yavaş bir

WAN'a geçer



8.2 IPv4 Paketi

IPv4 Paket Başlığı

IPv4 ağ katmanı için birincil iletişim protokolüdür.

Ağ başlığının bir çok amacı vardır:

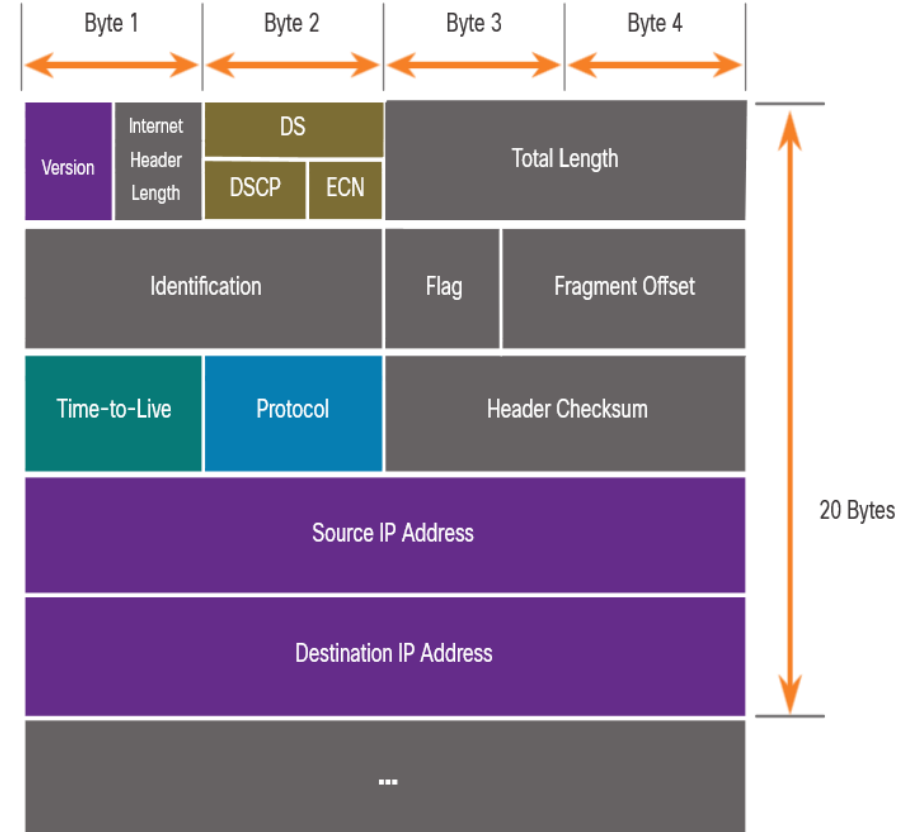
- Paketin doğru yönde (hedefe) gönderilmesini sağlar.
- Çeşitli alanlarda ağ katmanı işlemesi için bilgiler içerir.
- Başlıktaki bilgiler, paketi işleyen tüm katman 3 cihazları tarafından kullanılır

IPv4 Paket Başlık Alanları

IPv4 ağ başlığı özellikleri:

- İkili durumdadır.
- Birkaç bilgi alanı içerir.
- Diyagram soldan sağa, satır başına 4 bayt okunur.
- En önemli iki alan kaynak ve hedeftir.

Protokollerin bir veya daha fazla işlevi olabilir.



IPv4 Paket Başlık Alanları

IPv4 başlığındaki önemli alanlar:

Fonksiyon	Açıklama
Sürüm (Versiyon)	Bu, v6'nın aksine v4 için 4 bitlik bir alan = 0100 olacaktır
Farklılaştırılmış Hizmetler	QoS için kullanılır: DiffServ - DS alanı veya daha eski IntServ - ToS veya Hizmet Türü
Başlık Kontrolü (Header Checksum)	IPv4 başlığındaki bozulmayı tespit eder
Yaşam Süresi (Time to Live - TTL)	Katman 3 atlama sayısı. Sıfır olduğunda, yönlendirici paketi atar
Protokol	Bir sonraki seviye protokolü tanımlar: ICMP, TCP, UDP, vb.
Kaynak IPv4 Adresi	32-bit kaynak adresi
Hedef IPV4 Adresi	32-bit kaynak adresi

Video – Wireshark'ta Örnek IPv4 Başlıkları

Bu video aşağıdakileri kapsayacaktır:

- Wireshark'ta IPv4 Ethernet paketleri
- Kontrol bilgileri
- Paketler arasındaki fark

8.3 IPv6 Paketleri

IPv4'ün Sınırlamaları

IPv4'ün üç ana sınırlaması vardır:

IPv4 adres tükenmesi – Temelde IPv4 adreslememiz bitmiştir.

- Uçtan uca bağlantı eksikliği - IPv4'ün bu kadar uzun süre dayanmasını sağlamak için özel adresleme ve NAT oluşturulmuştu. Bu, genel adresleme ile doğrudan iletişimlerini sona erdirdi.
- Artan ağ karmaşıklığı - NAT, geçici çözüm olarak oluşturulmuştu ve ağ üstbilgilerinin adreslemesini değiştirmenin bir yan etkisi olarak ağda sorunlar yaratmaktadır. NAT, gecikmeye ve sorun giderme sorunlarına neden olur.

IPv6'ya Genel Bakış

- IPv6 Internet Engineering Task Force (IETF) tarafından geliştirilmiştir.
- IPv6, IPv4'ün sınırlamalarının üstesinden gelir.
- IPv6'nın sağladığı iyileştirmeler:
 - **Artan adres alanı** - 32-bit yerine 128-bit adrese göre
 - **İyileştirilmiş paket işleme** - daha az alan içeren basitleştirilmiş başlık
 - **NAT ihtiyacını ortadan kaldırır** - çok fazla adresleme olduğundan, dahili olarak özel adresleme kullanmaya ve paylaşılan bir genel adrese eşlenmeye gerek yoktur

IPv4 and IPv6 Address Space Comparison

Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^3	1,000
1 Million	10^6	1,000,000
1 Billion	10^9	1,000,000,000
1 Trillion	10^{12}	1,000,000,000,000
1 Quadrillion	10^{15}	1,000,000,000,000,000
1 Quintillion	10^{18}	1,000,000,000,000,000,000
1 Sextillion	10^{21}	1,000,000,000,000,000,000,000
1 Septillion	10^{24}	1,000,000,000,000,000,000,000,000
1 Octillion	10^{27}	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^{30}	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^{33}	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^{36}	1,000,000,000,000,000,000,000,000,000,000,000,000

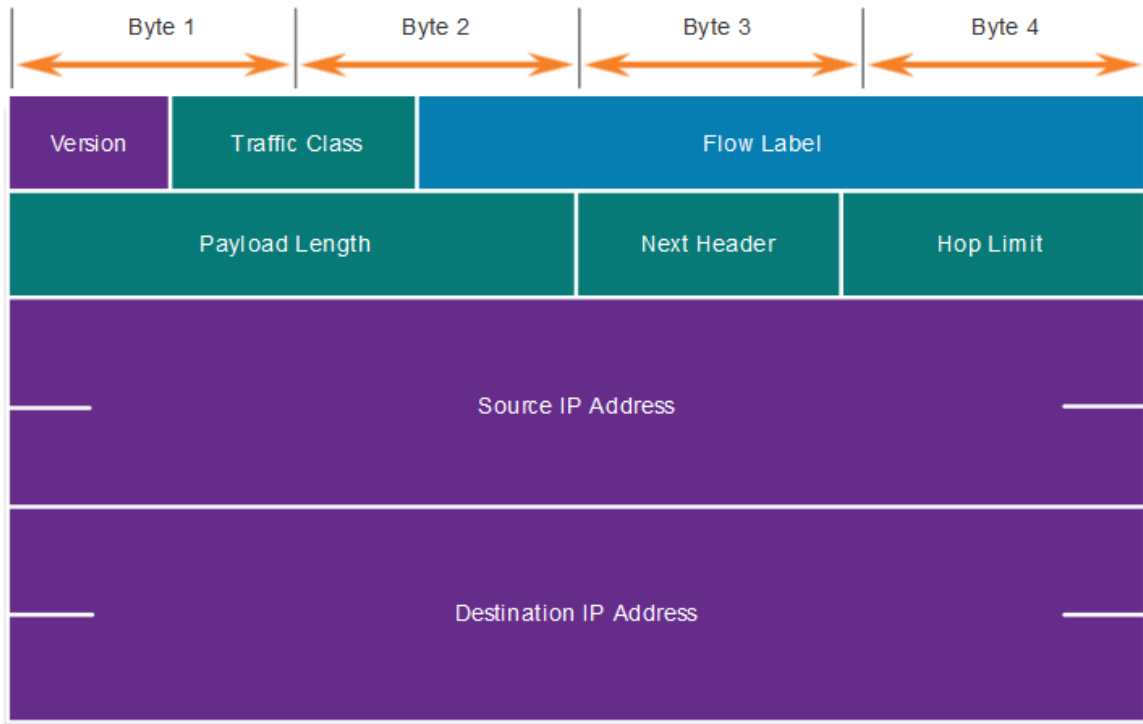
Legend

There are 4 billion IPv4 addresses

There are 340 undecillion IPv6 addresses

IPv6 Paket Başlığındaki IPv4 Paket Başlığı Alanları

- IPv6 başlığı basitleştirilmiştir, ancak daha küçük değildir.
- Başlık, 40 Bayt veya sekizli uzunluğunda sabitlenmiştir.
- Performansı artırmak için birkaç IPv4 alanı kaldırılmıştır.
- Performansı artırmak için bazı IPv4 alanları kaldırıldı::
 - Bayrak (Flag)
 - Parça Numarası (Fragment Offset)
 - Başlık Kontrolü (Header Checksum)



IPv6 Paket Başlıkları

IPv6 başlığındaki önemli alanlar:

Fonksiyon	Açıklama
Sürüm (Versiyon)	Bu, v6'da v4'ün aksine, 4 bitlik bir alan = 0110 olacaktır.
Trafik Sınıfı	QoS için kullanılır: DiffServ'e eşdeğer - DS alanı
Akış Etiketi	Aygıta aynı akış etiketlerini aynı şekilde, 20 bitlik alanla işlemlerini bildirir
Yük Boyutu	Bu 16 bitlik alan, IPv6 paketinin veri kısmının veya yükünün uzunluğunu gösterir
Sonraki Başlık	Bir sonraki seviye protokolü tanımlar: ICMP, TCP, UDP, vb.
Sıçrama Limiti	TTL alanı Katman 3 atlama sayısını değiştirir
Kaynak IPv4 Adresi	128- bit kaynak adresi
Hedef IPV4 Adresi	128-bit hedef adresi

IPv6 Paket Başlığı (devamı)

Pv6 paketi ayrıca uzantı başlıkları (EH) içerebilir.

EH başlıklarının özellikleri:

- isteğe bağlı ağ katmanı bilgisi sağlar
- isteğe bağlıdır
- IPv6 başlığı ile yük arasına yerleştirilir
- parçalanma, güvenlik, mobilite desteği vb. için kullanılabilir.

Not: IPv4'ün aksine, yönlendiriciler IPv6 paketlerini parçalamaz.

Video – Wireshark'ta Örnek IPv6 Başlıkları

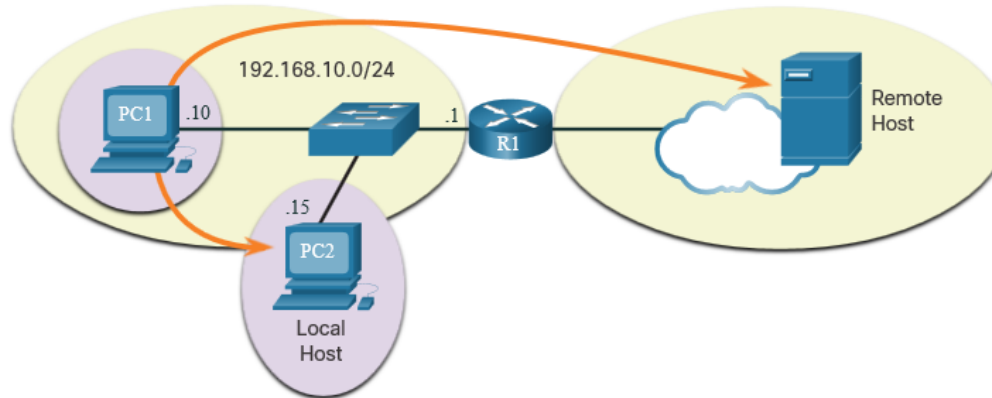
Bu video aşağıdakileri kapsayacaktır:

- Wireshark'ta IPv6 Ethernet paketleri
- Kontrol bilgileri
- Paketler arasındaki fark

8.4 Host Nasıl Yönlendirilir

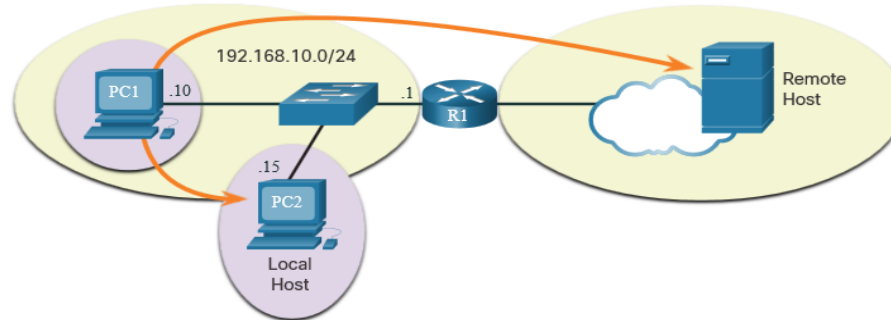
Host Yönlendirme Kararı

- Paketler her zaman kaynaktan oluşturulur.
- Her host kendi yönlendirme tablosunu oluşturur
- Bir host aşağıdakilere paket gönderebilir:
 - Kendisi – 127.0.0.1 (IPv4), ::1 (IPv6)
 - Yerel Hostlar – hedef aynı LAN üzerindedir
 - Uzak Hostlar – cihazlar aynı LAN üzerinde değildir



Host Yönlendirme Kararı (devamı)

- Kaynak cihaz hedefin yerel mi yoksa uzak mı olduğunu belirler
- Belirleme yöntemi:
 - IPv4 –Kaynak, hedef IP adresiyle birlikte kendi IP adresini ve Alt ağ maskesini kullanır
 - IPv6 – Kaynak, yerel yönlendirici (router) tarafından tanıtılan ağ adresini ve ön eki kullanır
- Yerel trafik, bir aracı cihaz tarafından işlenmek üzere ana bilgisayar arayüzünden atılır.
- Uzak trafik doğrudan LAN üzerindeki varsayılan ağ geçidine iletilir.



Varsayılan Ağ Geçidi

Bir yönlendirici veya katman 3 switch, varsayılan bir ağ geçidi olabilir.

Varsayılan bir ağ geçidinin (DGW) özellikleri:

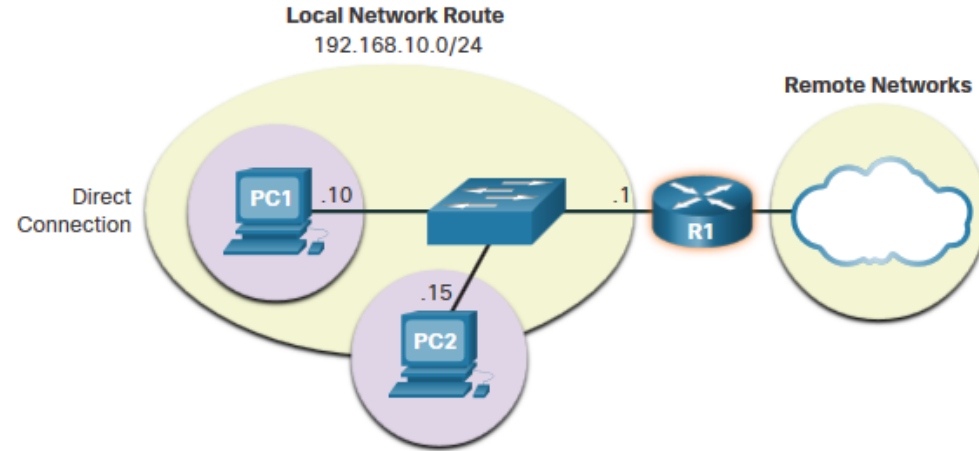
LAN'ın geri kalanıyla aynı aralıkta bir IP adresine sahip olmalıdır.

- LAN'dan veri kabul edebilir ve LAN üzerinden trafiği iletebilir.
- Diğer ağlara yönlendirilebilir.

Bir aygıtın varsayılan ağ geçidi yoksa veya kötü bir varsayılan ağ geçidi yoksa, trafiği LAN'ı terk edemez.

Host Varsayılan Ağ Geçidine Yönlendirir

- Host varsayılan ağ geçidini (DGW) statik olarak veya IPv4'teki DHCP aracılığıyla bilecektir.
- IPv6, DGW'yi bir yönlendirici talebi (router solicitation - RS) aracılığıyla gönderir veya manuel olarak yapılandırılabilir.
- DGW, yönlendirme tablosundaki son çare yolu olacak statik yoldur.
- LAN üzerindeki tüm aygıtlar, trafiği uzaktan göndermeyi planlıyorlarsa, router'ın DGW'sine ihtiyaç duyacaktır.



Host Yönlendirme Tablosu

- Windows'ta, PC yönlendirme tablosunu görüntülemek için print veya netstat -r'yi yönlendirin
- Bu iki komutla görüntülenen üç bölüm:
 - Arayüz Listesi - tüm potansiyel arayüzler ve MAC adresleme
 - IPv4 Yönlendirme Tablosu
 - IPv6 Yönlendirme Tablosu



IPv4 Routing Table for PC1

```
C:\Users\PC1> netstat -r
```

IPv4 Route Table

=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	25
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
	192.168.10.0	255.255.255.0	On-link	192.168.10.10	281
	192.168.10.10	255.255.255.255	On-link	192.168.10.10	281
	192.168.10.255	255.255.255.255	On-link	192.168.10.10	281
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
	224.0.0.0	240.0.0.0	On-link	192.168.10.10	281
	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
	255.255.255.255	255.255.255.255	On-link	192.168.10.10	281

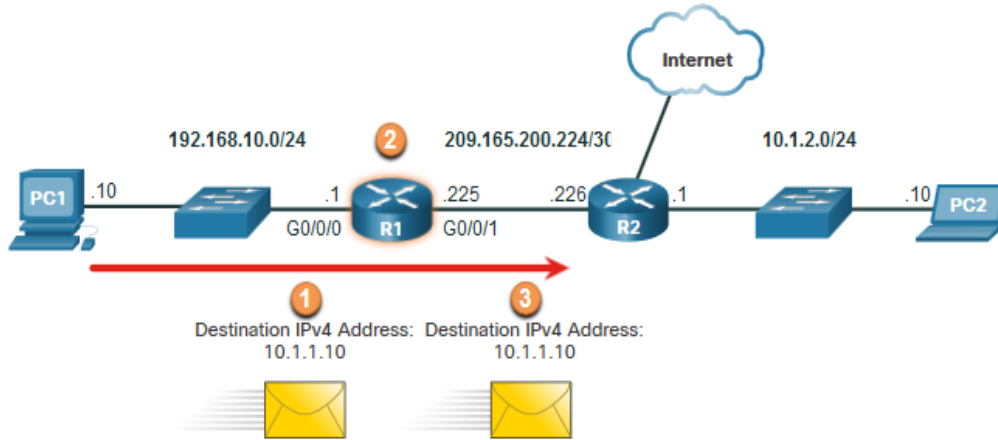
8.5 Yönlendirmeye (Routing)

Giriş

Yönlendirmeye Giriş

Router Paket Yönlendirme Kararı

Router çerçeveyi ana cihazdan aldığı anda ne olur?



R1 Routing Table

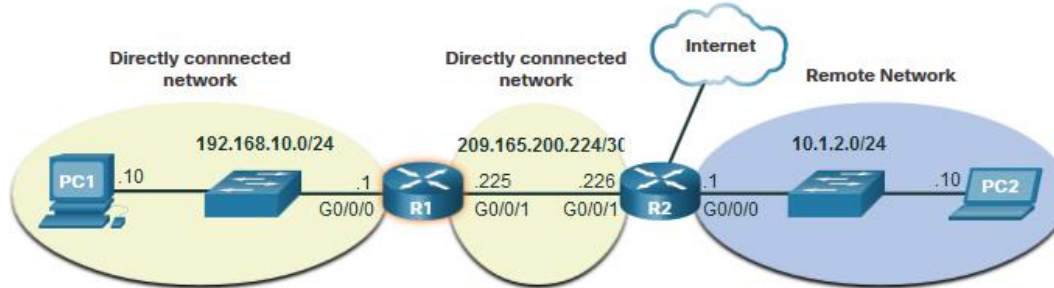
Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	via R2
Default Route 0.0.0.0/0	via R2

1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

IP Router Yönlendirme Tablosu

Bir router'ın yönlendirme tablosunda üç tür yol vardır:

- **Doğrudan Bağlı** - Arayüzün etkin olması ve adresleme içermesi şartıyla, bu rotalar router tarafından otomatik olarak eklenir.
- **Uzak** - Bunlar, yönlendiricinin doğrudan bağlantıya sahip olmadığı ve öğrenilebilen rotalardır:
 - Manuel olarak – statik bir rotayla
 - Dinamik olarak – routerların bilgilerini birbirleriyle paylaşmasını sağlamak için bir yönlendirme protokolü kullanarak
- **Varsayılan Rota** – bu, yönlendirme tablosunda bir eşleşme olmadığında tüm trafiği belirli bir yöne yönlendirir

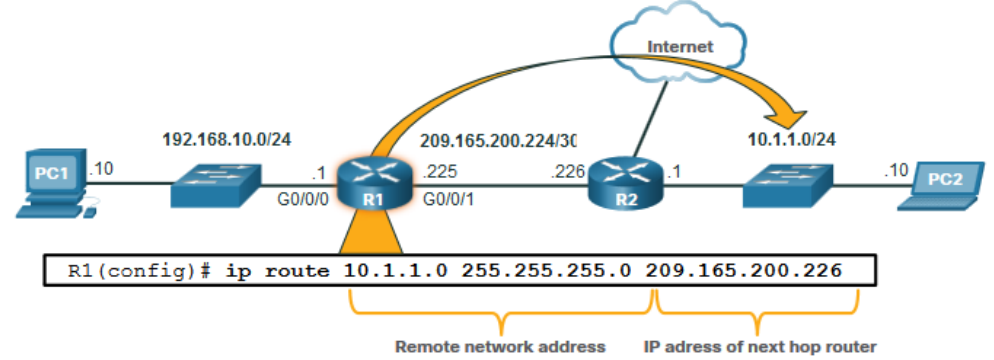


Yönlendirmeye Giriş

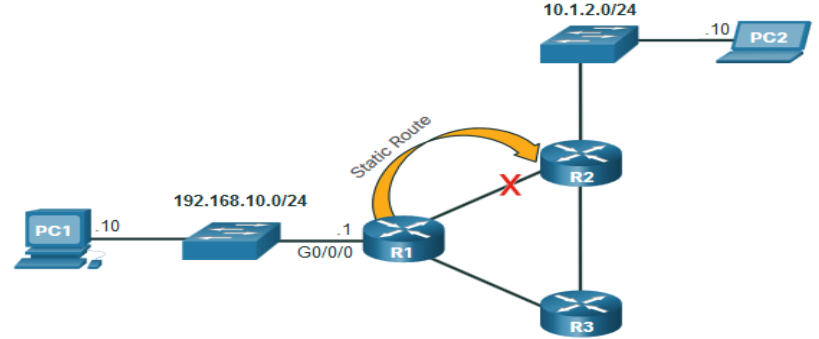
Statik Yönlendirme

Statik Yönlendirme Özellikleri:

- Manuel olarak yapılandırılmalıdır
- Topolojide bir değişiklik olduğunda yönetici tarafından manuel olarak ayarlanmalıdır
- Küçük yedekli olmayan ağlar için uygundur
- Genellikle bir varsayılan yolu yapılandırmak için dinamik bir yönlendirme protokolüyle birlikte kullanılır



R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.



If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

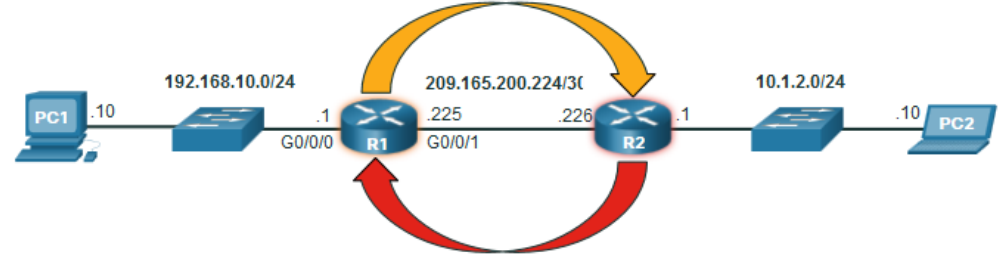
Yönlendirmeye Giriş

Dinamik Yönlendirme

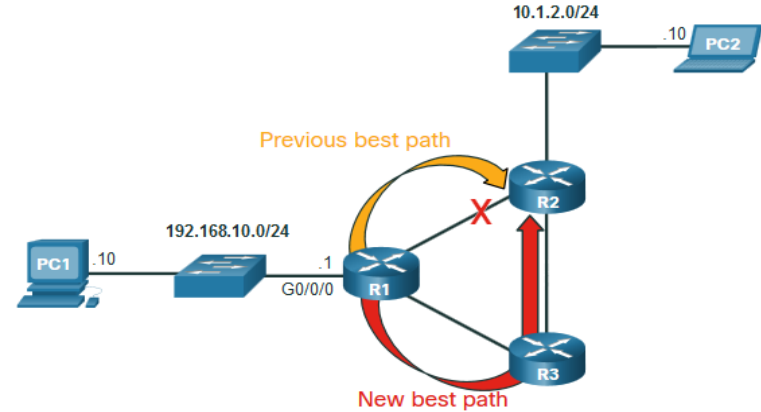
Dinamik rotalar otomatik olarak:

- Uzak ağları keşfeder
- Güncel bilgileri korur
- Hedefe giden en iyi yolu seçer
- Topoloji değişikliği olduğunda en iyi yeni yolları bulur

Dinamik yönlendirme, statik varsayılan yolları diğer yönlendiricilerle de paylaşabilir.



- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.



R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

Video – IPv4 Router Yönlendirme Tabloları

Bu video, IPv4 router yönlendirme tablosundaki bilgileri açıklayacaktır.

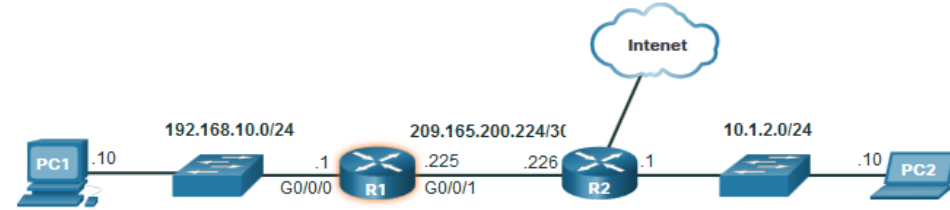
IPv4 Yönlendirme Tablolarına Giriş

Show ip route komutu aşağıdaki yönlendirme kaynaklarını gösterir:

- **L** - Doğrudan bağlı yerel arayüz IP adresi
- **C** – Doğrudan bağlı ağ
- **S** – Statik yol bir yönetici tarafından manuel olarak yapılandırıldı
- **O** – OSPF
- **D** – EIGRP

Bu komut rota türlerini gösterir:

- Doğrudan bağlantılı – C ve L
- Uzak Rotalar– O, D, vb.
- Varsayılan Rotalar– S*



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O      10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L      192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L      209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

8.6 Modül Pratiği ve Quiz

Bu modülde ne öğrendim?

- IP bağlantısızdır, en iyi çabadır ve medyadan bağımsızdır.
- IP, paket teslimini garanti etmez.
- IPv4 paket başlığı, paketle ilgili bilgileri içeren alanlardan oluşur.
- IPv6, IPv4'ün uçtan uca bağlantı eksikliğinin ve artan ağ karmaşıklığının üstesinden gelir.
- Bir cihaz, bir hedefin kendisi mi, başka bir yerel ana bilgisayar (local host) ve uzak bir ana bilgisayar (remote host) mı olduğunu belirleyecektir.
- Varsayılan bir ağ geçidi, LAN'ın bir parçası olan ve diğer ağlara açılan bir kapı olarak kullanılacak olan yönlendiricidir.
- Yönlendirme tablosu, bilinen tüm ağ adreslerinin (önekler) ve paketin nereye yönlendirileceğinin bir listesini içerir.
- Yönlendirici en uzun alt ağ maskesini veya önek eşleşmesini kullanır.
- Yönlendirme tablosunun üç tür yol girişi vardır: doğrudan bağlı ağlar, uzak ağlar ve varsayılan yol.

